PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-007849
(43)Date of publication of application : 12.01.2001

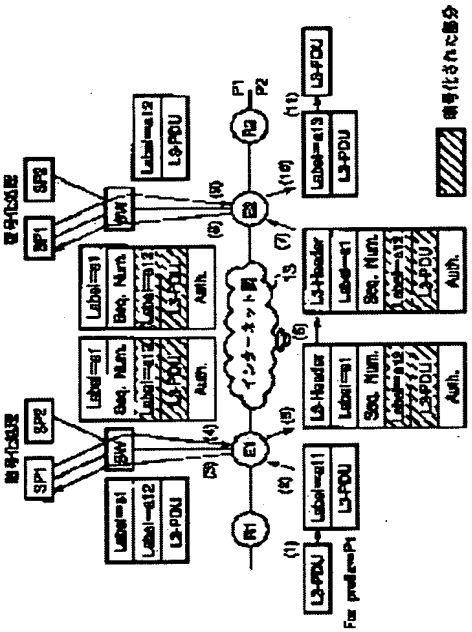
(51)Int.CI. H04L 12/56
H04L 9/10
H04L 12/46
H04L 12/28
H04L 12/66

(21)Application number : 11-173022
(22)Date of filing : 18.06.1999

(71)Applicant : TOSHIBA CORP
(72)Inventor : NOGAMI KAZUO
OBA YOSHIHIRO
KISHIGAMI TORU

(54) MPLS PACKET PROCESSING METHOD AND MPLS PACKET PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an MPLS packet processing method that can support an MPLS security function even in the case that one node supports an IP encapsulation or a plurality of VPNs realized by an LSP of the MPLS.
SOLUTION: A label switch path is set between two nodes that support a label switch, either of the two nodes encrypts a packet and uses the label switch path to transmit an encrypted packet, the other decodes the encrypted packet received on the label switch path in this encrypted packet processing method adopting a multi-protocol label switch(MPLS), where information relating to packet security association is used for the label of the MPLS to transmit packets.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－7849
（P2001－7849A）
(43)公開日　平成13年１月12日(2001.1.12)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ 12/56		Ｈ０４Ｌ 11/20	１０２Ａ	５Ｊ１０４
9/10		9/00	６２１Ｚ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｂ	
12/66				

審査請求　未請求　請求項の数12　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－173022

(22)出願日　平成11年６月18日(1999.6.18)

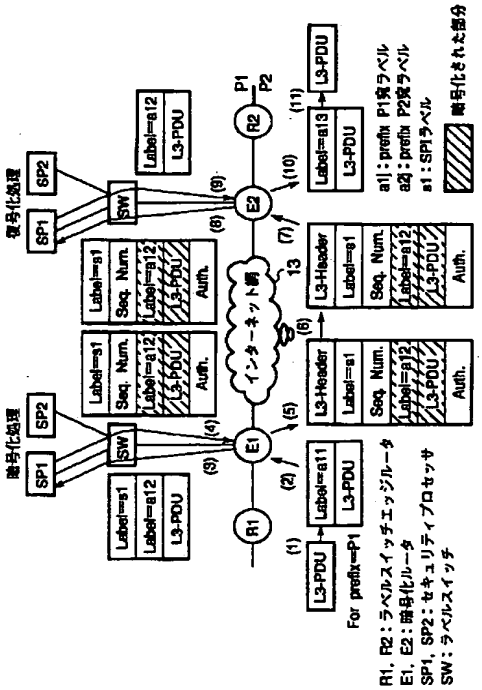
特許法第64条第２項ただし書の規定により図面第17図の一部は不掲載とした。

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　野上　和男
東京都日野市旭が丘３丁目１番地の１　株式会社東芝日野工場内
(72)発明者　大場　義洋
東京都日野市旭が丘３丁目１番地の１　株式会社東芝日野工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　ＭＰＬＳパケット処理方法及びＭＰＬＳパケット処理装置

(57)【要約】
【課題】１つのノードがＩＰカプセル化あるいは、ＭＰＬＳのＬＳＰで実現される複数のＶＰＮをサポートする場合でも、ＭＰＬＳセキュリティ機能をサポートすることができるＭＰＬＳのパケット処理方法を提供する。
【解決手段】ラベルスイッチをサポートする２つのノードの間にラベルスイッチングパスが設定されており、２つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング（ＭＰＬＳ）の暗号化パケット処理方法であって、パケットのセキュリティアソシエーションに関する情報を、ＭＰＬＳのラベルとして用いてパケットの送信を行うようにする。



【特許請求の範囲】
【請求項１】 ラベルスイッチをサポートする２つのノードの間にラベルスイッチングパスが設定されており、２つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理方法であって、
パケットのセキュリティアソシエーションに関する情報を、ＭＰＬＳのラベルとして用いてパケットの送信を行うようにしたことを特徴とするＭＰＬＳパケット処理方法。
【請求項２】 前記セキュリティアソシエーションに関する情報を表すラベルを含むパケットをレイヤ３パケットにカプセル化したことを特徴とする請求項１記載のＭＰＬＳパケット処理方法。
【請求項３】 上記セキュリティアソシエーションに関する情報を表わすラベルのラベル値として、暗号化しないパケットに対して割り当てるラベル値とは異なる値を使用し、両者のラベル値の相違により暗号化するパケットと暗号化しないパケットを区別するようにしたことを特徴とする請求項１記載のＭＰＬＳパケット処理方法。
【請求項４】 送信されるパケットは、レイヤ３パケットと複数のラベルスタックエントリからなるラベルスタックを含み、上記ノードがレイヤ３パケットを暗号化して送信する場合には、セキュリティアソシエーションに関する情報をを含むラベルスタックエントリに対しては上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオンにし、上記ノードがＭＰＬＳパケットを暗号化して送信する場合には、上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオフにすることを特徴とする請求項１又は３記載のＭＰＬＳパケット処理方法。
【請求項５】 上記セキュリティアソシエーションに関する情報を表わすラベルにおいて、そのラベル値に応じて異なる暗号処理プロセッサを用いて並列処理を行うようにしたことを特徴とする請求項１～４のいずれか１つに記載のＭＰＬＳパケット処理方法。
【請求項６】 上記暗号処理プロセッサは、上記ノードの外部に当該ノードとは別体で設けられていることを特徴とする請求項５記載のＭＰＬＳパケット処理方法。
【請求項７】 上記暗号化処理プロセッサを切り換えるために、上記暗号処理プロセッサと上記ノードとの間に設けられたスイッチをさらに有し、このスイッチは、ラベルスイッチと、イーサスイッチ等の通常のスイッチのいずれかであることを特徴とする請求項１～６のいずれか１つに記載のＭＰＬＳパケット処理方法。
【請求項８】 上記暗号化パケット処理は、パケットの暗号化と認証のうち少なくともどちらか一方を行うことを特徴とする請求項１～７のいずれか１つに記載のＭＰＬＳパケット処理方法。
【請求項９】 上記ノードは複数のＶＰＮトンネルをサポートする暗号化パケット処理ノードであり、ＶＰＮトンネルがＩＰカプセル化のトンネルかＭＰＬＳのトンネルかに応じて適切なパケットフォーマットを選択するようにしたことを特徴とする請求項１～８のいずれか１つに記載のＭＰＬＳパケット処理方法。
【請求項１０】 ラベルスイッチをサポートする２つのノードの間にラベルスイッチングパスが設定されており、２つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理装置であって、
パケットのセキュリティアソシエーションに関する情報を表すラベルをＭＰＬＳのラベルとして、暗号化されたレイヤ３パケットにカプセル化して送信する送信処理部と、
上記ラベルスイッチングパスを介して受信したパケットのセキュリティアソシエーションに関する情報に対応する暗号化方法を用いて受信パケットを復号する受信処理部と、
を具備することを特徴とするＭＰＬＳパケット処理装置。
【請求項１１】 ラベルスイッチをサポートする２つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理方法であって、
上記ラベルスイッチングパスの始点において、受信したレイヤ３パケットに、ＭＰＬＳのラベルを含むパケットをカプセル化して転送することを特徴とするＭＰＬＳパケット処理方法。
【請求項１２】 ラベルスイッチをサポートする２つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理装置であって、
上記ラベルスイッチングパスの始点において、レイヤ３パケットに、ＭＰＬＳのラベルを含むパケットをカプセル化して転送する転送処理部を有することを特徴とするＭＰＬＳパケット処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】ＭＰＬＳパケット処理方法及びＭＰＬＳパケット処理装置に関するものである。
【０００２】
【従来の技術】近年インターネットを使い、企業ネットワークを構築するＶＰＮ（Virtual Private Network ）が注目されている。特定のサイト間でのＩＰコネクティビティを、別のＩＰネットワーク（プロバイダネットワ

ーク）を用いて実現するＶＰＮ（Virtual Private Network ）においては、コネクティビティを確保するサイト間でＶＰＮ内を流れるパケットをプロバイダネットワーク上に通すための「ＶＰＮトンネル」を生成する必要がある。このとき、サイトとプロバイダネットワークとの境界ルータがＶＰＮトンネルのエンドポイントとなる。この境界ルータを「ＶＰＮエッジノード」とよぶ。ＶＰＮトンネル内を流れるＩＰパケットは、プロバイダネットワークを流れるＩＰパケットにカプセル化（ＩＰカプセル化）されるか、あるいはＭＰＬＳ（Multi-Protocol Label Switching）のＬＳＰ（Label Switched Path ）を用いて実現される。一般に、プロバイダネットワークには、不特定多数のユーザがアクセス可能である。このため、ＶＰＮトンネルを流れるパケットの盗聴、改ざん等を防ぐためにＶＰＮトンネルを流れるパケットに対して何らかのセキュリティ処理を施すことによりセキュアなＶＰＮ通信を確保する必要がある。セキュリティ処理には、暗号化と認証がある。

【０００３】送信者が間違いなく本人であることを確認し他人による「なりすまし」を防止する認証機能や、通信データを暗号化して他人からのデータの盗み見やデータの改ざんを防止する暗号化機能をＩＰパケットに提供する技術として、ＩＰＳＥＣがある。

【０００４】図１８にＩＰＳＥＣゲートウェイ（ＩＰＳＥＣ－ＧＷ）によるＩＰＳＥＣ処理の仕組みを示す。そのメカニズムは以下の通りである。

【０００５】１．端末Ａから端末Ｂ宛にＩＰパケットを送り出す。

【０００６】２．ＩＰＳＥＣ－ＧＷはセキュリティ・ポリシー・データベース５０とＳＡデータベース５１を保持しており、入力された各パケットに対して、これらのデータベースを検索してＩＰＳＥＣの処理方法を調べる。まず、セキュリティ・ポリシーデータベース５０を検索してＩＰＳＥＣ処理の有無を判定し、該当するＳＡ（Security Association）を調べる。ＳＡがない場合にはＩＳＡＫＭＰ（InternetSecurity Association and Key Management Protocol ）を使用してＳＡを確立する。

【０００７】３．同様にしてＳＡデータベース５１を検索する。ＳＡデータベース５１を検索すると当該ＳＡに対応するＩＰＳＥＣの処理方法、例えばヘッダ種類、モード、アルゴリズムなどを調べることができる。

【０００８】４．この後、ＩＰＳＥＣ－ＧＷは、ＩＰＳＥＣ（暗号化されたＩＰパケット）を送り出す。すなわち、ＳＡで指示された暗号化などの処理方法に従って暗号化などを実行してＩＰＳＥＣヘッダをつけてインターネット網１０２にパケットを送り出す。

【０００９】５．受信側のＩＰＳＥＣ－ＧＷはセキュリティ・ポリシー・データベース５０’とＳＡデータベース５１’を保持しており、入力された各パケットに対して、これらのデータベースを検索してＩＰＳＥＣの処理方法を調べる。ここではＩＰＳＥＣパケットを受信するとＩＰＳＥＣヘッダ中のＳＰＩ（Security Parameter Index）を調べる。

【００１０】６．次にＳＡデータベース５１’を検索し、ＳＰＩ値をもとに復号処理方法などを調べる。

【００１１】７．ＩＰＳＥＣ－ＧＷはＩＰＳＥＣ処理を行った後、ＩＰＳＥＣヘッダを取り除いて端末Ｂ宛にパケットを送信する。

【００１２】図１９に、ＩＰＳＥＣ用のＳＡ確立と鍵交換にかかわるＩＳＡＫＭＰ（Internet Security Association and Key Management Protocol ）を示す。

【００１３】１．ＩＳＡＫＭＰフェーズの最初では、ＩＳＡＫＭＰで使用するＳＡ（ISAKMP-SA ）をまず確立する。つまりこれから行うやり取りのためにお互いを認証しＩＳＡＫＭＰ用の鍵をやりとりする、

２．そしてＩＳＡＫＭＰの次フェーズに移り、ＩＰＳＥＣで使用するＳＡ（IPSEC-SA）を確立する。

【００１４】３．鍵交換フェーズに入る。このフェーズではＯａｋｌａｙプロトコルを利用してＩＰＳＥＣ用の鍵を交換する。鍵交換にはＯａｋｌａｙプロトコルをＩＳＡＫＭＰプロトコル上で使用する。ここでＩＳＡＫＭＰの目的はＩＰＳＥＣ用のＳＡの確立と鍵交換にある。ＩＳＡＫＭＰは鍵交換プロトコルでなく鍵交換プロトコルを利用するためのペイロードを提供している。実際の鍵交換はＯａｋｌａｙプロトコルを用いている。

【００１５】図２０はトランスポートモードとトンネルモードの各々における、ＩＰパケット中のＡＨおよびＥＳＰヘッダ位置と、認証／暗号化範囲を示す図である。ＡＨ及びＥＳＰのＳＰＩフィールドとシーケンス番号フィールドの位置は同じである。すなわち、１．トランスポートモードでは、オリジナルのＩＰヘッダの直後に位置し、２．トンネルモードではオリジナルのＩＰヘッダと新ＩＰヘッダとの間に位置する。ＥＳＰのパディングデータや次ヘッダフィールド、認証データ用フィールドはパケットの後ろのフィールドに位置する。ＥＳＰの場合、暗号化範囲はいずれのモードでも同じで、シーケンス番号の直後から認証データの直前までであり、認証範囲はＡＨとＥＳＰとでは異なっている。ＡＨではＩＰヘッダの中の固定フィールドまで認証範囲とするのに対して、ＥＳＰではＩＰヘッダは認証範囲にしていない。

【００１６】図２１にＡＨ（Authentication Header ）の構造を示す。ＡＨは送信者が間違いなく本人であることを認証するためのヘッダである。外部からのリプレイ攻撃を阻止するためにシーケンス番号が割り当ててある。なお、ＡＨはＩＰパケットヘッダの直後に現れる。

【００１７】図２２にＥＳＰ（Encapsulating Security Payload）の構造を示す。ＩＰパケットまたはＩＰパケットからＩＰヘッダを除いたＩＰデータグラム部を暗号化してカプセル化し、ペイロード・データ部に埋め込

む。送信者が本人であることを認証する機能もある。

【００１８】

【発明が解決しようとする課題】上記した方法でＩＰにカプセリングされたＩＰＳＥＣのパケットを処理（IP in IP）する場合、ルータはトンネルの入り口でＬ３フォワーディングテーブルのベストマッチ検索を２回行なう必要がある。つまり１回目は出口ルータを求めるために、２回目はその出口ルータへのNext Hopルータを求めるためである。したがって、このような検索処理によりルータの負荷が増大してしまうという問題があった。

【００１９】一方、インターネット技術の標準化組織であるＩＥＴＦで標準化されているＭＰＬＳ（Multi-Protocol Label Switching）を用いることにより、ＶＰＮ（Virtual Private Network ）を構築することが可能である。しかしながら、ＶＰＮトンネルをＭＰＬＳで実現する場合に、セキュリティ処理のための具体的な機構が何ら考えられていなかった。したがって、１つのノードがＩＰカプセル化あるいは、ＭＰＬＳのＬＳＰで実現される複数のＶＰＮをサポートする場合には、ＭＰＬＳセキュリティ機能をサポートすることができなかった。

【００２０】本発明はこのような課題に着目してなされたものであり、その目的とするところは、１つのノードがＩＰカプセル化あるいは、ＭＰＬＳのＬＳＰで実現される複数のＶＰＮをサポートする場合でも、ＭＰＬＳセキュリティ機能をサポートすることができるＭＰＬＳパケット処理方法及びＭＰＬＳパケット処理装置を提供することにある。

【００２１】また、本発明の他の目的は、カプセル化ノードにおいて、宛先アドレスに関するベストマッチ検索を１回に減らすことができるＭＰＬＳパケット処理方法及びＭＰＬＳパケット処理装置を提供することにある。

【００２２】

【課題を解決するための手段】上記の目的を達成するために、第１の発明は、ラベルスイッチをサポートする２つのノードの間にラベルスイッチングパスが設定されており、２つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理方法であって、パケットのセキュリティアソシエーションに関する情報を、ＭＰＬＳのラベルとして用いてパケットの送信を行うようにする。

【００２３】また、第２の発明は、第１の発明において、前記セキュリティアソシエーションに関する情報を表すラベルを含むパケットをレイヤ3パケットにカプセル化する。

【００２４】また、第３の発明は、第１の発明において、上記セキュリティアソシエーションに関する情報を表わすラベルのラベル値として、暗号化しないパケットに対して割り当てるラベル値とは異なる値を使用し、両者のラベル値の相違により暗号化するパケットと暗号化しないパケットを区別する。

【００２５】また、第４の発明は、第１または第３の発明において、送信されるパケットは、レイヤ３パケットと複数のラベルスタックエントリからなるラベルスタックを含み、上記ノードがレイヤ３パケットを暗号化して送信する場合には、セキュリティアソシエーションに関する情報を含むラベルスタックエントリに対しては上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオンにし、上記ノードがＭＰＬＳパケットを暗号化して送信する場合には、上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオフにする。

【００２６】また、第５の発明は、第１～第４のいずれか１つの発明において、上記セキュリティアソシエーションに関する情報を表わすラベルにおいて、そのラベル値に応じて異なる暗号処理プロセッサを用いて並列処理を行うようにする。

【００２７】また、第６の発明は、第５の発明において、上記暗号処理プロセッサは、上記ノードの外部に当該ノードとは別体で設けられている。

【００２８】また、第７の発明は、第１～第６のいずれか１つの発明において、上記暗号化処理プロセッサを切り換えるために、上記暗号処理プロセッサと上記ノードとの間に設けられたスイッチをさらに有し、このスイッチは、ラベルスイッチと、イーサスイッチ等の通常のスイッチのいずれかである。

【００２９】また、第８の発明は、第１～第７のいずれか１つの発明において、上記ＭＰＬＳパケット処理は、パケットの暗号化と認証のうち少なくともどちらか一方を行う。

【００３０】また、第９の発明は、第１～第８のいずれか１つの発明において、上記ノードは複数のＶＰＮトンネルをサポートする暗号化パケット処理ノードであり、ＶＰＮトンネルがＩＰカプセル化のトンネルかＭＰＬＳのトンネルかに応じて適切なパケットフォーマットを選択する。

【００３１】また、第１０の発明は、ラベルスイッチをサポートする２つのノードの間にラベルスイッチングパスが設定されており、２つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理装置であって、パケットのセキュリティアソシエーションに関する情報を表すラベルをＭＰＬＳのラベルとして、暗号化されたレイヤ３パケットにカプセル化して送信する送信処理部と、上記ラベルスイッチングパスを介して受信したパケットのセキュリティアソシエーション

に関する情報に対応する暗号化方法を用いて受信パケットを復号する受信処理部とを具備する。

【００３２】また、第１１の発明は、ラベルスイッチをサポートする２つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理方法であって、上記ラベルスイッチングパスの始点において、受信したレイヤ３パケットに、ＭＰＬＳのラベルを含むパケットをカプセル化して転送する。

【００３３】また、第１２の発明は、ラベルスイッチをサポートする２つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング（ＭＰＬＳ）のパケット処理装置であって、上記ラベルスイッチングパスの始点において、レイヤ3パケットに、ＭＰＬＳのラベルを含むパケットをカプセル化して転送する転送処理部を有する。

【００３４】

【発明の実施の形態】まず、本発明の実施形態に係る暗号化パケット処理方法の概略を説明する。図１（ａ）はＭＰＬＳのフォーマットを示す図であり、Ｌ２ヘッダ１００、シムヘッダ（Ｓｈｉｍヘッダ）１０１、Ｌ３ヘッダ１０２、Ｌ４ヘッダ１０３、データ１０４からなる。

【００３５】上記シムヘッダ１０１は、図１（ｂ）に示すような、３２ビットのラベルスタックエントリ（２０ビットのラベル１０５、３ビットのエクスペリメンタルユース１０６、Ｓフラグ１０７、８ビットのＴＴＬ１０８からなる）を複数個並べたラベルスタックとなっている。ラベル１０５はパケット転送用またはＳＡラベルとして用いられ、これらのラベル値を異ならせることにより両者を区別できる。

【００３６】また、複数個のラベルスタックエントリのうち、最後のエントリ以外のＳフラグは０（オフ）となっており、最後のエントリのＳフラグは１（オン）となっている。これによりラベルスタックの最後のエントリであるかどうかはＳフラグの状態により判別することができる。Ｌ２ヘッダ１００に隣接する第１のラベルスタックはパケット転送用のエントリである。本実施形態ではこのエントリと隣り合う第２のラベルスタックエントリのラベル１０５に上記したＩＰＳＥＣで用いたＳＰＩに対応するＳＡラベル情報（例えば後述するＬａｂｅｌ＝ｓ１）を挿入して送信する。

【００３７】本実施形態では、ＩＰカプセル化あるいは、ＭＰＬＳのＬＳＰで実現される複数のＶＰＮトンネルをサポートするノードにおいて、パケットが転送されるＶＰＮに対して以下の２つの適切な処理方式のいずれかを選択する手段を有する。

【００３８】（第１の処理方式）ＩＰカプセル化で実現される１つ以上のＶＰＮトンネルをサポートするノードにおいて、パケットが転送されるＶＰＮに対して以下の第１の処理方式を使用する手段を有する。すなわち、ＶＰＮトンネルをＩＰカプセル化で実現し、必要に応じて、各ＶＰＮサイトで、パケットにＭＰＬＳラベルを付与した上で、レイヤ３（Ｌ３）のＩＰヘッダ（外部ＩＰヘッダ）をつけてＩＰ網を通過する機構を設ける。したがって、ＶＰＮトンネルを流れるパケットおよびＭＰＬＳラベルの情報は、Ｌ３パケットにカプセリングされている。通常のトンネルモードのＩＰｓｅｃと同様に内部ＩＰヘッダも含めて暗号化を行う。また、暗号化されるパケットはＩＰパケットでなくてもよく、ＭＰＬＳのＳｈｉｍヘッダがついたＩＰパケットであってもよい。つまり、外部ＩＰヘッダをつけることによりＶＰＮの出口までパケットが転送できる。ＳＡを表すための情報として本処理方式では、ＳＡを表す情報がエンコードされるラベル（ＳＡラベル）を定義する。

【００３９】ＶＰＮトンネルの入口側ルータでは、ＶＰＮトンネルにパケットを暗号化して送信する場合には、暗号化されたパケットに、ＳＡラベル、ＬＳＰ上のラベルスイッチングに使用されるラベル（トンネル出口ラベル）、の順にラベルスタックエントリをプッシュして送信する。ＳＡラベルには、（セキュリティプロトコル、ＳＰＩ）をマッピングさせる。

【００４０】ＳＡとＳＡラベルとのマッピングをＶＰＮトンネルの両端のルータで行う必要があるが、この方法として、（ｉ）両端のルータでマッピングを手動設定する方法と、（ii）ＩＳＡＫＭＰ（Internet Security Association and Key Management Protocol ）などのプロトコルを用いて自動的に設定する方法の２種類がある。

【００４１】暗号化されるパケットがＩＰパケットである場合には、ＳＡラベルが入れられるラベルスタックエントリ中のラベルスタックの最後のエントリであることを示すフラグ（Ｓフラグ）をオンにする。

【００４２】暗号化されるパケットがＭＰＬＳのラベル化パケットである場合には、ＳＡラベルが入れられるラベルスタックエントリ中のＳフラグをオフにする。

【００４３】また、ＶＰＮトンネルを流れるパケットを暗号化しない場合には、ＳＡラベルをつけないようにする。暗号化されないＩＰパケットがＶＰＮトンネルを流れる場合には、トンネルの出口ラベルに対するラベルスタックエントリのＳフラグがオンになる。暗号化されないＭＰＬＳのラベル化パケットがＶＰＮトンネルを流れる場合には、トンネル出口ラベルに対するラベルスタックエントリのＳフラグがオフになる。

【００４４】このとき、次のラベルスタックエントリが存在するが、このラベルはＳＡラベルではない。したがって、トンネル出口ラベルの次のラベルとして、ＳＡラベルがくる場合と、通常のラベルスイッチに使用されるラベル（パケット転送ラベル）がくる場合がある。そこでこれらを区別する必要があるため、ＳＡラベルと、パケット転送ラベルとでは異なるラベル値を割当てるようにする。

【００４５】ＶＰＮトンネルの出口側ルータでは、ＶＰＮトンネルからパケットを受信すると、外部ＩＰヘッダを取り外し、先頭のトンネル出口ラベルをポップする。ポップした結果がＩＰパケットであれば、このＩＰパケットがセキュリティポリシー的に転送可能かどうかを判断し、転送可能であれば通常のＩＰ転送を行い、転送が禁止されていれば直ちに廃棄する。

【００４６】ポップした結果、次のラベルスタックエントリがあれば、もし、このエントリのラベルがＳＡラベルであるかどうかの判定を行う。もし、ＳＡレベルでなくパケット転送ラベルであれば、ラベル値を元にセキュリティポリシー的に転送可能かどうかのチェックを行う。そして転送可能であれば、ラベルスイッチングによる転送を行い、転送が禁止されていれば、直ちに廃棄する。一方、ＳＡラベルであれば、ＳＡラベルをつけたまま受信パケットを暗号処理部に転送し、復号化処理を行う。

【００４７】暗号処理部でパケットの復号化を行う場合には、ＳＡラベル値にマッチするＳＡを決定し、マッチしたＳＡに対応する暗号化アルゴリズム、鍵情報を用いて復号化を行う。

【００４８】復号化処理後、ＳＡラベルが入っているラベルスタックエントリのＳフラグがオフであれば、復号化したパケットをＩＰパケットとして転送し、Ｓフラグがオンであれば、復号化したパケットをＭＰＬＳのラベル化パケットとして転送する。

【００４９】（第２の処理方式）第２の処理方式ではＶＰＮトンネルをＭＰＬＳのＬＳＰで実現する。このときＶＰＮトンネルを流れるパケットは、ＩＰカプセル化の場合と同様に、内部ＩＰヘッダも含めて暗号化が可能である。また、暗号化されるパケットはＩＰパケットでなくてもよく、ＭＰＬＳのＳｈｉｍヘッダがついたＩＰパケットであってもよい。ただし、第１の処理方式（ＩＰカプセル化）の場合と異なり、外部ＩＰヘッダはつけないようにする。

【００５０】外部ＩＰヘッダをつけないため、ＳＡを表すための情報が別に必要になる。そこで本処理方式では、ＳＡを表す情報がエンコードされるラベル（ＳＡラベル）を定義する。

【００５１】ＶＰＮトンネルの入口側ルータでは、ＶＰＮトンネルにパケットを暗号化して送信する場合には、暗号化されたパケットに、ＳＡラベル、ＬＳＰ上のラベルスイッチングに使用されるラベル（トンネル出口ラベル）、の順にラベルスタックエントリをプッシュして送信する。

【００５２】ＳＡラベルには、（トンネル出口の宛先アドレス情報、セキュリティプロトコル、ＳＰＩ）をマッピングさせる。また、トンネル出口ラベルをトンネル出口の宛先アドレス情報として使用する場合には、ＳＡラベルには、（セキュリティプロトコル、ＳＰＩ）をマッピングさせ、トンネル出口ラベルとＳＡラベルの組によりＳＡを決定することも可能である。

【００５３】ＳＡとＳＡラベルとのマッピングをＶＰＮトンネルの両端のルータで取る必要があるが、この方法として、（ｉ）両端のルータでマッピングを手動設定する方法と、（ii）ＩＳＡＫＭＰ（Internet Security Association and Key Management Protocol ）などのプロトコルを用いて自動的に設定する方法の２種類がある。

【００５４】暗号化されるパケットがＩＰパケットである場合には、ＳＡラベルが入れられるラベルスタックエントリ中のラベルスタックの最後のエントリであることを示すフラグ（Ｓフラグ）をオンにする。

【００５５】暗号化されるパケットがＭＰＬＳのラベル化パケットである場合には、ＳＡラベルが入れられるラベルスタックエントリ中のＳフラグをオフにする。

【００５６】また、ＶＰＮトンネルを流れるパケットを暗号化しない場合には、ＳＡラベルをつけないようにする。暗号化されないＩＰパケットがＶＰＮトンネルを流れる場合には、トンネルの出口ラベルに対するラベルスタックエントリのＳフラグがオンになる。暗号化されないラベル化パケットがＶＰＮトンネルを流れる場合には、トンネル出口ラベルに対するラベルスタックエントリのＳフラグがオフになる。

【００５７】このとき、次のラベルスタックエントリが存在するが、このラベルはＳＡラベルではない。したがって、トンネル出口ラベルの次のラベルとして、ＳＡラベルがくる場合と、通常のラベルスイッチに使用されるラベル（パケット転送ラベル）がくる場合があり、これらを区別する必要がある。そこでここではＳＡラベルと、パケット転送ラベルとでは異なるラベル値を割当てるようにする。

【００５８】ＶＰＮトンネルの出口側ルータでは、ＶＰＮトンネルからパケットを受信すると、先頭のトンネル出口ラベルをポップする。ポップした結果が、ＩＰパケットであれば、セキュリティポリシー的にこのＩＰパケットが転送可能であるかどうかを判断する。転送可能であれば通常のＩＰ転送を行い、転送が禁止されていれば、直ちに廃棄する。

【００５９】ポップした結果、次のラベルスタックエントリがあれば、もし、このエントリのラベルがＳＡラベルであるかどうかの判定を行う。もし、ＳＡラベルではなくパケット転送ラベルであれば、ラベル値を元にセキュリティポリシー的に転送可能かどうかのチェックを行い、転送可能であれば、ラベルスイッチングによる転送を行い、転送が禁止されていれば、直ちに廃棄する。一方、もし、ＳＡラベルであれば、ＳＡラベルをつけたまま受信パケットを暗号処理部に転送し、復号化処理を行う。

【００６０】暗号処理部でパケットの復号化を行う場合には、ＳＡラベル値にマッチするＳＡを決定し、マッチ

したＳＡに対応する暗号化アルゴリズム、鍵情報を用いて復号化を行う。

【００６１】復号化処理後、ＳＡラベルが入っているラベルスタックエントリのＳフラグがオフであれば、復号化したパケットをＩＰパケットとして転送し、Ｓフラグがオンであれば、復号化したパケットをＭＰＬＳのラベル化パケットとして転送する。

【００６２】なお、ＶＰＮエッジルータと暗号処理部は同じ機器にある必要はなく、別々の機器であってもよい。さらに、別々の機器の場合には、暗号処理部は、ネットワークインターフェースを持った暗号処理機器としてＶＰＮエッジルータとネットワークを介して接続していてもよい。また、この場合には、暗号処理機器とＶＰＮエッジルータの間のパケット転送をラベルスイッチにより実現してもよく、その際ＳＡラベルを用いてパケットをラベルスイッチしてもよい。

【００６３】暗号処理部は、複数の暗号処理プロセッサから構成してもよい。ＶＰＮエッジルータは、ＳＡラベルを参照して、複数の暗号処理プロセッサのいずれかに処理を振り分けることにより暗号処理の負荷分散を行ってもよい。ただし、負荷分散を行う場合には、パケットの順序逆転が起こらないように暗号化時にパケットのヘッダ情報を参照してパケットとＳＡのマッピングを決める必要がある。

【００６４】以下、図面を参照して本発明の実施形態を詳細に説明する。

【００６５】（第１実施形態）図２に、１つのノードがＩＰカプセル化（第１の処理方式）で１つ以上のＶＰＮを構築する場合のネットワークの構成を示す。この図においては、Ｅ１－Ｅ２間のＶＰＮを転送されるパケットはＩＰカプセル化され、宛先ＩＰアドレスにより中継先が判定される。

【００６６】図３に本実施形態の方式による暗号化処理を行うＶＰＮの一例を示す。

【００６７】図３において、Ｅ１，Ｅ２はＶＰＮエッジルータ（暗号化ルータ）、Ｒ１，Ｒ２はＶＰＮサイト内のラベルスイッチエッジルータ（Ｒ１，Ｒ２は異なるＶＰＮサイトに属する）、ＳＰ１，ＳＰ２はセキュリティプロセッサ、ＳＷはラベルスイッチである。本実施形態では、セキュリティプロセッサＳＰ１，ＳＰ２と、ＶＰＮエッジルータＥ１，Ｅ２が別機器になっており、かつそれらはラベルスイッチＳＷにより接続されている場合を示す。Ｐ１，Ｐ２はＲ２が属するＶＰＮサイト内に存在するネットワークアドレスプレフィクスである。

【００６８】まず、Ｒ１が所属するＶＰＮサイト内の図示されないホストから送信された宛先アドレスがＰ１にマッチするパケット（Ｌ３－ＰＤＵ）をＲ１が受信する（１）。

【００６９】Ｒ１では、Ｐ１に対して出力ラベル＝ａ１１を割り当てているとすると、受信パケットに出力ラベル＝ａ１１のラベルスタックエントリをプッシュしてＥ１に送信する。このとき、Ｓフラグはオンにする（２）。

【００７０】Ｅ１はこのパケットを受信する。Ｅ１では、入力ラベル＝ａ１１に対応して出力ラベルにラベルａ１２を割り当てており、さらに、パケットをＳＡラベル＝ｓ１を用いて暗号化するように設定されているとする。このときＥ１は、受信パケットに出力ラベル＝ａ１２のラベルスタックエントリをプッシュし、次にＳＡラベル＝ｓ１のラベルスタックエントリをプッシュしてラベルスイッチＳＷを経由してセキュリティプロセッサＳＰ１に送る。

【００７１】ラベルスイッチＳＷは、入力ＳＡラベル＝ｓ１と、必要であればパケットのＬ２送信元アドレスも参照してパケットのラベルスイッチングを行い、ＳＰ１にパケットを転送する（２），（３）。

【００７２】ＳＰ１はＳＡラベルｓ１をポップし、ｓ１に対応するＳＡが使用する暗号化アルゴリズム、鍵を用いてパケットを暗号化して、再びＳＡラベルｓ１をプッシュしてＳＷ経由でＥ１に送信する（４）。このとき、暗号化されるパケットには、リプレイアタックを防ぐためのシーケンス番号（Seq. Num. ）、および、認証のための情報（Auth. ）を付加してもよい。

【００７３】Ｅ１は、受信したパケットのＳＡラベルを参照することによりトンネルの出口のＶＰＮエッジルータＥ２を得る。Ｅ１において、Ｅ２に対するトンネル出口はＥ２であるため、Ｅ２のＩＰアドレスをＩＰヘッダの宛先ＩＰアドレスに入れ、ＳＡラベル＝ｓ１をＬ３＿ＰＤＵにカプセリングしてインターネット網１３に送信する（５）。

【００７４】インターネット１３はこのパケットを受信する。このとき、受信パケットのＩＰヘッダの宛先アドレスを見て中継処理が行われ、受信パケットはＥ２に送信される（６）。

【００７５】Ｅ２はこのパケットを受信すると、受信パケットのＩＰヘッダを見て、先頭のラベルスタックＳＡラベル＝ｓ１を参照して、ラベルスイッチＳＷ経由でセキュリティプロセッサＳＰ１にパケットを送信する（７），（８）。

【００７６】ＳＰ１はＳＡラベルｓ１をポップし、ｓ１に対応するＳＡが使用する暗号化アルゴリズム、鍵を用いてパケットを復号して、復号後のパケットの先頭のラベルスタックエントリ中のラベル値＝ａ１３を参照してＳＷ経由でＥ２に送信する（９）。

【００７７】Ｅ２はこのパケットを受信すると、受信パケットの先頭ラベルスタックエントリをポップする。ポップされたラベルスタックエントリ中の入力ラベル値ａ１２には、出力ラベル値＝ａ１３が対応したとすると、Ｅ２はパケットに出力ラベル値＝ａ１３が指定されるパケットラベルスタックエントリをプッシュして、Ｒ２に

送信する（１０）。

【００７８】Ｒ２は受信パケットの先頭ラベルスタックエントリのＬａｂｅｌ＝ａ１３をポップし、得られたＩＰパケットを通常のＩＰ転送でサイト内の図示されない次段ルータに送信する（１１）。

【００７９】（第２実施形態）以下に本発明の第２実施形態を説明する。第２実施形態では、ＭＰＬＳのＬＳＰによりＶＰＮトンネルを実現した場合の処理方式（第２の処理方式）を説明する。

【００８０】図４にＭＰＬＳを用いた暗号化処理を行うＶＰＮの一例を示す。

【００８１】図４において、Ｅ１，Ｅ２はＶＰＮエッジルータ（暗号化ルータ）、Ｒ１，Ｒ２はＶＰＮサイト内のラベルスイッチエッジルータ（Ｒ１，Ｒ２は異なるＶＰＮサイトに属する）、Ａはプロバイダネットワーク内ルータ、ＳＰ１，ＳＰ２はセキュリティプロセッサ、ＳＷはラベルスイッチである。本実施形態では、セキュリティプロセッサとＶＰＮエッジルータが別機器になっており、かつそれらはラベルスイッチＳＷにより接続されている場合を示す。Ｐ１，Ｐ２はＲ２が属するＶＰＮサイト内に存在するネットワークアドレスプレフィクスである。

【００８２】まず、Ｒ１が所属するＶＰＮサイト内の図示されないホストから送信された宛先アドレスがＰ１にマッチするパケットをＲ１が受信する（１）。

【００８３】Ｒ１では、Ｐ１に対して出力ラベル＝ａ１１を割り当てているとすると、受信パケットに出力ラベル＝ａ１１のラベルスタックエントリをプッシュしてＥ１に送信する（２）。このとき、Ｓフラグはオンにする。

【００８４】Ｅ１はこのパケットを受信する。Ｅ１では、入力ラベル＝ａ１１に対応して出力ラベルに対してラベルａ１２を割り当てており、さらに、パケットをＳＡラベル＝ｓ１を用いて暗号化するように設定されているとする。このときＥ１は、受信パケットに出力ラベル＝ａ１２のラベルスタックエントリをプッシュし、次にＳＡラベル＝ｓ１のラベルスタックエントリをプッシュしてラベルスイッチＳＷを経由してセキュリティプロセッサＳＰ１に送る。

【００８５】ラベルスイッチＳＷは、入力ＳＡラベル＝ｓ１と、必要であればパケットのＬ２送信元アドレスも参照してパケットのラベルスイッチングを行い、ＳＰ１にパケットを転送する（２），（３）。

【００８６】ＳＰ１はＳＡラベルｓ１をポップし、ｓ１に対応するＳＡが使用する暗号化アルゴリズム、鍵を用いてパケットを暗号化して、再びＳＡラベルｓ１をプッシュしてＳＷ経由でＥ１に送信する（４）。このとき、暗号化されるパケットには、リプレイアタックを防ぐためのシーケンス番号（Seq. Num. ）、および、認証のための情報（Auth. ）を付加してもよい。

【００８７】Ｅ１は、受信したパケットのＳＡラベルを参照することによりトンネルの出口のＶＰＮエッジルータＥ２を決める。Ｅ１において、Ｅ２に対するトンネル出口ラベル＝ｂ１とすると、Ｅ１は受信パケットに出力ラベル＝ｂ１のラベルスタックエントリをプッシュしてプロバイダネットワークＡに送信する（５）。

【００８８】Ａはこのパケットを受信する。このとき、受信パケットの入力ラベル＝ｂ１に対して出力ラベル＝ｂ２を割り当てているとすると、Ａは受信パケットの入力ラベルスタックエントリをラベル＝ａ１１のラベルスタックエントリにスワップしてＥ２に送信する（６）。

【００８９】Ｅ２はこのパケットを受信すると、受信パケットの先頭のラベルスタックエントリをポップする。次に、ＳＡラベル＝ｓ１を参照して、ラベルスイッチＳＷ経由でセキュリティプロセッサＳＰ１にパケットを送信する（７），（８）。

【００９０】ＳＰ１はＳＡラベルｓ１をポップし、ｓ１に対応するＳＡが使用する暗号化アルゴリズム、鍵を用いてパケットを復号して、復号後のパケットの先頭のラベルスタックエントリ中のラベル値＝ａ１３を参照してＳＷ経由でＥ１に送信する（９）。

【００９１】Ｅ２はこのパケットを受信すると、受信パケットの先頭ラベルスタックエントリをポップする。ポップされたラベルスタックエントリ中の入力ラベル値ａ１２には、出力ラベル値＝ａ１３が対応したとすると、Ｅ２はパケットに出力ラベル値＝ａ１３が指定されるパケットラベルスタックエントリをプッシュして、Ｒ２に送信する（１０）。

【００９２】Ｒ２は受信パケットの先頭ラベルスタックエントリをポップし、得られたＩＰパケットを通常のＩＰ転送でサイト内の図示されない次段ルータに送信する（１１）。

【００９３】（第３実施形態）以下に本発明の第３実施形態を説明する。図５に上記したＩＰネットワークとＭＰＬＳネットワークが混在し、１つのノードがＩＰカプセル化及び、ＭＰＬＳのＬＳＰでＶＰＮを構築する場合のネットワークの構成を示す。図５においては、Ｅ１－Ｅ２間のＶＰＮを転送されるパケットはＩＰカプセル化され、宛先ＩＰアドレスにより中継先が判定されている。また、Ｅ１－Ｅ３間のＶＰＮを転送されるパケットはＭＰＬＳラベルが付加され、ＭＰＬＳラベルにより中継先が判定されている。

【００９４】Ｅ１においては、ＩＰカプセル化によるＶＰＮとＭＰＬＳのＬＳＰによるＶＰＮをサポートする必要がある。したがってＥ１ではまず初めにパケットが転送されるＶＰＮトンネルにより、上記の２つの処理方式のいずれかを選択する。

【００９５】図６は、この２つの処理方式のいずれかを選択する工程を示すフローチャートである。ＶＰＮトンネルの送信側のノードにおいては、受信したパケットの

宛先アドレスと当該パケットが転送されるＶＰＮがＩＰカプセル化により実現されるのか、ＭＰＬＳのＬＳＰにより実現されるのかを対応づけるテーブルを用意し、このテーブルを参照することでいずれの処理方式を選択する。

【００９６】一方、ＶＰＮトンネルの受信側のノードにおいては、図５のようなＩＰ，ＭＰＬＳ混在のネットワーク構成において、ポート毎にＶＰＮトンネルの種類が異なっているのであれば、受信パケットが到着したポートとそのポートがサポートするＶＰＮの種類を予め対応づけておけば良い。

【００９７】ステップＳ１の判断により受信パケットが転送されるＶＰＮトンネルがＭＰＬＳかどうかを判断し、ＭＰＬＳである場合にはステップＳ２のパケット受信処理（ＭＰＬＳラベル化パケット）を行い、ＭＰＬＳでない場合にはステップＳ３のパケット受信処理（ＩＰパケット）を行う。各受信処理の詳細は上記した通りである。

【００９８】（第４実施形態）以下に本発明の第４実施形態を説明する。図７に本実施形態を用いたＶＰＮエッジルータが、ＩＰパケットを受信した場合の処理を説明するためのフローチャートを示す。

【００９９】受信パケットヘッダをＨ、Ｈ中のプロトコル番号をＰｒ、Ｈ中の宛先アドレスをＤとする（ステップＳ１０）。次のステップＳ１１でＤが自ノードアドレスの一つと一致するかどうかを判断し、もし、Ｄが自ノードアドレスの一つと一致していなければ、後述する暗号側処理１（ステップＳ１４）を行う。Ｄが自ノードアドレスの一つと一致している場合には次のステップＳ１２でＰｒがＥＳＰまたはＡＨであるかどうかを判断し、もし、ＰｒがＥＳＰまたはＡＨのいずれでもなければ後述する暗号側処理１（ステップＳ１４）を行い、ＰｒがＥＳＰまたはＡＨのいずれかであれば、後述する復号側処理１（ステップＳ１３）を行う。

【０１００】図８に本実施形態のＶＰＮエッジルータが、ＭＰＬＳのラベル化パケットを受信した場合の処理を説明するためのフローチャートを示す。

【０１０１】まずステップＳ２０で、受信パケットの先頭ラベルスタックエントリのラベル値をＬｉとし、このＬｉに対応するＶＰＮ内のパケット転送に使用される出力ラベル（トンネル外出力ラベル）をＬｏとする。

【０１０２】次のステップＳ２１では、先頭のラベルスタックエントリをポップし、ポップしたラベルスタックエントリ中のラベル値をｓ１とし、ポップ後のパケットをＰとする。次のステップＳ２２においてＬｏ＝Ｎｕｌｌかどうかを判断し、もし、ＬｏがＮｕｌｌでなければ、後述する暗号側処理２（ステップＳ２６）を行い処理を終了する。もし、ＬｏがＮｕｌｌであれば、ステップＳ２３でｓ１＝Ｎｕｌｌかどうかを判断し、ｓ１がＮｕｌｌでなければ後述する復号側処理２（ステップＳ２５）を行って処理を終了し、ｓ１がＮｕｌｌであればＰはＩＰパケットであるため、ステップＳ２４でＰを通常のＩＰ転送により次段ルータに送信して処理を終了する（次段ルータが自ルータであればＰのＩＰヘッダを取り除いて所定の上位レイヤアプリケーションに渡す）。

【０１０３】図９に暗号側処理１の詳細を説明するためのフローチャートを示す。

【０１０４】まず、受信パケットのペイロードをＰとし（ステップＳ３０）、次のステップＳ３１で受信パケットの宛先アドレスＤに対するトンネル出口ルータのアドレスをＥ２、Ｅ２への次段ルータに対する出力インターフェースアドレスをＥ１とする。次にステップＳ３２で受信パケットのヘッダＨにベストマッチするセレクタをＳとし、このＳに対するセキュリティポリシーをＰｏとする。

【０１０５】次のステップＳ３４でＰｏにて示されるセキュリティポリシーが非暗号化、廃棄、暗号化のどれであるかを判断し、セキュリティポリシーが非暗号化であれば、Ｐ′：＝Ｐとし（ステップＳ３５）、Ｐ′を宛先アドレスＥ２、送信元アドレスＥ１のＩＰパケットにカプセル化して送信し（ステップＳ３９）、処理を終了する。

【０１０６】一方、ステップＳ３４の判断においてセキュリティポリシーが廃棄であれば、Ｐを直ちに廃棄して処理を終了する（ステップＳ３３）。一方、Ｐｏにて示されるセキュリティポリシーが暗号化であれば、ステップＳ３６でＳに対するセキュリティプロトコルをＰｒとするとともに、Ａ：＝（Ｓ，Ｅ２，Ｐｒ）とし、次のステップＳ３７でＡが使用するＳＰＩをＩとする。次にステップＳ３８で、Ｐを、Ａに対する暗号化アルゴリズムおよび鍵を用いて暗号化し、暗号化されたパケットをＰ′とし、次のステップＳ３９でＰ′を宛先アドレスＥ２、送信元アドレスＥ１のＩＰパケットにカプセル化して送信し、処理を終了する。

【０１０７】図１０に復号側処理１の詳細を説明するためのフローチャートを示す。まずステップＳ４０で、受信パケットのペイロードをＰとし、受信パケットの宛先アドレスＤに対するトンネル出口ルータのアドレスをＥ２、Ｐに対するセキュリティプロトコルをＰｒとする。次のステップＳ４１では、Ｐに対するＳＰＩをＩ、Ａ：＝（Ｉ，Ｅ２，Ｐｒ）、Ｉが使用するセキュリティプロセッサ（ＳＰ）の番号をＭとする。

【０１０８】次にステップＳ４２で、ＰをＡに対する復号化アルゴリズムおよび鍵を用いて番号ＭのＳＰで復号化し、復号化されたパケットをＰ′とする。次のステップＳ４３で復号化に成功したかどうかを判断し、もし、復号化に失敗すれば、直ちにＰ′を廃棄（ステップＳ４６）して処理を終了する。そうでなければ、以下の処理を行う。

【０１０９】すなわち、ステップＳ４４に進んでＩに対

するセキュリティデータベースのセレクタをSとする。また、P′にベストマッチするセレクタをS′とする。さらに、Sに対するセキュリティポリシーをPoとする。

【0110】次にステップS45に進んでSとS′が一致し、かつPoが暗号化であるかどうかを判断し、もし、SとS′が一致しないかまたはPoが暗号化でない場合には、直ちにP′を廃棄（ステップS46）して処理を終了する。そうでない場合には、P′を次段ルータに送信（ステップS47）して処理を終了する。

【0111】図11に、暗号側処理2の詳細を説明するためのフローチャートを示す。

【0112】まずステップS50で、入力側ラベルLiに対するトンネル出口ルータのアドレスをE2とし、次のステップS51でLiにベストマッチするセキュリティデータベースのセレクタをSとするとともに、Sに対するセキュリティポリシーをPoとする。次にステップS53でPoにて示されるセキュリティポリシーが非暗号化、廃棄、暗号化のどれであるかを判断し、セキュリティポリシーが非暗号化であれば、P′：＝Pとし（ステップS54）、ステップS59に移行してP′にs1をプッシュして宛先アドレスE2のIPパケットにカプセル化して送信し、処理を終了する。

【0113】一方、ステップS53においてPoにて示されるセキュリティポリシーが廃棄であれば、Pを直ちに廃棄（ステップS52）して処理を終了する。一方、ステップS53においてPoにて示されるセキュリティポリシーが暗号化であれば、ステップS55でSに対するセキュリティプロトコルをPrとし、A：＝（S，E2，Pr）とし、次のステップS56でAが使用するSPIラベルをs1とする。

【0114】次に、Pの先頭のラベルスタックエントリのラベル値をLoとし（ステップS57）、次のステップS58でPをAに対する暗号化アルゴリズムおよび鍵を用いて暗号化し、暗号化されたパケットをP′とする。次にステップS59でP′にs1をプッシュして、宛先アドレスE2、送信元アドレスE1のIPパケットにカプセル化して送信し、処理を終了する。

【0115】図12に復号側処理2の詳細を説明するためのフローチャートを示す。

【0116】まずステップS60で、ラベル値s1に対するプロトコルIDをPrとする。次にステップS61で、Prがセキュリティプロトコルを表わしているかどうかを判断し、Noであれば以下を実行する。

【0117】P′：＝Pとし（ステップS66）、P′にベストマッチするセキュリティデータベースのセレクタをS、Sに対するセキュリティポリシーをPoとする（ステップS67）。次にステップS68でPoが非暗号化であるかどうかを判断し、Poが非暗号化でなければ、直ちにP′を廃棄（ステップS71）して処理を終了する。そうでなければステップS69に進んで、s1がラベルスタックの最後のエントリのラベルであるかどうかをチェックする。ここでYESであればステップS73に進んで、P′を通常のIP転送により次段ルータに送信し（次段ルータが自ルータであればPのIPヘッダを取り除いて所定の上位レイヤアプリケーションに渡す）、そうでなければ、ステップS2に進んでLiをLoに書き換え、P′をLoに対する次段ルータに送信して処理を終了する。

【0118】一方、ステップS61においてPrがセキュリティプロトコルを表していれば、ステップS62に進んでPをs1に対する復号化アルゴリズムおよび鍵を用いて復号化し、復号化されたパケットをP′とする。

【0119】ステップS63で復号化に成功したかどうかを判断し、復号化に失敗すれば、直ちにP′を廃棄（ステップS71）して処理を終了する。そうでなければ、ステップS64に進んで、s1に対するセキュリティデータベースのセレクタをSとする。また、P′にベストマッチするセレクタをS′とする。また、Sに対するセキュリティポリシーをPoとする。

【0120】次にステップS65に進んで、S＝S′かつPoが暗号化であるかどうかを判断し、もし、SとS′が一致しないかまたはPoが暗号化でない場合には、直ちにP′を廃棄（ステップS1）して処理を終了する。そうでない場合にはステップS69に進んで、s1がラベルスタックの最後のエントリのラベルであるかどうかをチェックし、そうであればステップS73に進んで、P′を通常のIP転送により次段ルータに送信する（次段ルータが自ルータであればPのIPヘッダを取り除いて所定の上位レイヤアプリケーションに渡す）。また、最後のエントリのラベルでなければ、ステップS70に進んでP′の先頭ラベルをLiにして、Liに対するトンネル外出力ラベルをLoにする。次のステップS72で、LiをLoに書き換え、P′をLoに対する次段ルータに送信して処理を終了する。

【0121】図13に本実施形態で用いられるセキュリティデータベースの構成を示す。

【0122】図13においては、トンネル出口のVPNエッジルータがE2であるようなVPNトンネルを用いて転送されないパケットは廃棄される。

【0123】また、トンネル出口のVPNエッジルータがE2であるようなパケットのうち、パケットの送信元アドレスがH11であるようなパケットは、セキュリティプロトコルESP、暗号化アルゴリズムA1、鍵K1を用いて暗号化され、パケットの送信元アドレスがH12であるようなパケットは、セキュリティプロトコルE2、暗号化アルゴリズムA2、鍵K2を用いて暗号化され、パケットの送信元アドレスがH11，H12以外のパケットはそのまま送信される。

【0124】図14に本実施形態におけるVPNトンネ

ル上を転送されるパケットのパケットフォーマットを示す。

【０１２５】図１４において、トンネルＰＤＵ（ＩＰｖ４）はＶＰＮトンネル上を転送されるＩＰｖ４パケットを含むレイヤ２ヘッダ以下のＰＤＵであり、トンネルＰＤＵ（ＩＰ６４）はＶＰＮトンネル上を転送されるＩＰｖ６パケットを含むレイヤ２ヘッダ以下のＰＤＵである。また、［Ａ］はＡが省略可能であることを示し、｛Ａ｜｜Ｂ｝はＡ，Ｂのいずれか１つを選択することを示す。｛Ａ｜｜Ｂ｜｜Ｃ｝はＡ，Ｂ，Ｃのいずれか１つを選択することを示す。

【０１２６】図１５に、図７から図１２に示すフローチャートの処理を実現するノードのブロック図を示す。

【０１２７】ノードは、パケット入力部２０１、ＩＰ／ＭＰＬＳヘッダ解析部２０２、自ノード宛パケット処理部２００、暗号処理部２０６、復号処理部２０３、セキュリティデータベース（ＳＤ）２０４、暗号化側セキュリティポリシー決定部２０５、ＩＰ／ＭＰＬＳパケットフォワーディング処理部２０８、パケット出力部２０９、復号化側セキュリティポリシー決定部２０７から構成される。

【０１２８】ノードは、パケット入力部２０１からパケットを受信すると、ＩＰ／ＭＰＬＳヘッダ解析部２０２にて、パケットのＬ２ヘッダの情報を用いて、受信パケットがＩＰパケットかＭＰＬＳのラベル化パケットかを決定し、それぞれのパケットに依存したヘッダ処理を行う。

【０１２９】もし、受信パケットが自ノード宛のパケットであれば以下のいずれかが実行される。すなわち、ヘッダ情報からペイロードがセキュリティ処理されていることが判明すれば、復号処理部２０３にて復号処理を行う。そうでなければ、自ノード宛パケット処理部２００にて上位レイヤ処理を行う。

【０１３０】復号処理部２０３では、ＳＤ２０４を検索し、ＭＰＬＳのＳＡラベル値にマッチするエントリがあれば、そのエントリに対して使用される暗号化アルゴリズム、鍵を用いて、ペイロードの復号化処理を行う。次に、復号化側セキュリティポリシー決定部２０７において、復号化後により得られるＩＰパケットヘッダまたはＭＰＬＳヘッダと、ＳＤ２０４の内容とからパケットをフォワード可能かどうかを決定し、可能であれば、ＩＰ／ＭＰＬＳパケットフォワーディング処理部２０８にて出力インターフェースを決め、パケット出力部２０９からＩＰパケットまたはＭＰＬＳパケットを出力する。

【０１３１】一方、受信パケットが自ノード宛のパケットでなければ、暗号化側セキュリティポリシーにて、ＳＤ２０４の検索を行う。もし、受信ヘッダ情報にマッチするようなＳＤエントリがなければパケットを廃棄する。一方、そのようなＳＤエントリがある場合には以下のいずれかの処理を行う。

【０１３２】すなわち、パケットを暗号化する必要がなければ、ＩＰ／ＭＰＬＳフォワーディング処理部２０８にてＩＰヘッダまたはＭＰＬＳヘッダの情報から出力インターフェースを決め、パケット出力部２０９からパケットを出力する。一方、パケットを暗号化する必要があれば、暗号処理部２０６において、受信パケットにマッチしたＳＤ２０４のエントリにて指定される暗号化アルゴリズム鍵を用いてパケットの暗号化を行う。その際、ＩＰ／ＭＰＬＳフォワーディング処理部２０８にてＩＰヘッダまたはＭＰＬＳヘッダの情報から出力インターフェースを決め、パケット出力部２０９からパケットを出力する。

【０１３３】（第５実施形態）以下に本発明の第５実施形態を説明する。図１６に本実施形態で用いられる暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノード内に配置した場合のハード構成の一例を示す。

【０１３４】図１６において、暗号処理ノードは、スイッチ部３００、ネットワークインターフェース部３０１、内部処理インターフェース部３０３および、中央処理部（ＣＰＵ＋Ｍｅｍ）３０２から構成される。なお、スイッチ部３００を用いるかわりに、内部パスを用いることにより、スイッチ部、ネットワークインターフェース部、内部処理インターフェース部および、中央処理部間のデータ転送を実現してもよい。

【０１３５】各ネットワークインターフェース部３０１はセキュリティデータベース（ＳＤ）およびフォワーディングテーブル（ＦＷ）を持つ。また、各内部処理インターフェース部３０３は、セキュリティプロセッサ部（ＳＰ）およびフォワーディングテーブル（ＦＷ）を持つ。中央処理部３０２は、自ノード宛のＩＰパケットのうちペイロードがＩＰのＰＤＵでないもの（ＩＰ－ｉｎ－ＩＰでないもの）に対する処理および、ＦＷ，ＳＤ，ＳＰの管理を行う。

【０１３６】ノードは、パケットをネットワークインターフェース部３０１から受信した場合には、まず、受信パケットのＩＰヘッダまたはＭＰＬＳヘッダの情報からパケットが自ノード宛かどうかを調べ、一致しない場合には、以下の処理を行う。

【０１３７】まず、ネットワークインターフェース部３０１内のフォワーディングテーブル（ＦＷ）を参照してトンネル出口を決定する。次に、セキュリティデータベース（ＳＤ）を参照し、パケットに対してセキュリティ処理を行わない場合には、スイッチ部経由でトンネル出口に対する出力インターフェースにパケットを出力する。パケットに対して暗号化処理を行う場合には、ＳＡラベル、および処理すべき内部処理インターフェース部３０３を決定した後、パケットにトンネル出口ラベル、ＳＡラベル（暗号化の必要がなければＮｕｌｌが指定される）、の順にプッシュした後、これをスイッチ部３０

0を通して決定した内部処理インターフェース部303に送信する。

【0138】内部処理インターフェース部303では、まず、SAラベルをポップする。次に、ポップ後のパケットの先頭にあるトンネル出口ラベルをキーに内部処理インタフェース部303内のFWを参照して、指定されたトンネル出口に対する出力ネットワークインターフェース部を決定する。次に、SAラベルがNull でなければパケットをSPで暗号化処理後、スイッチ部300を通して出力ネットワークインターフェース部に送信する。出力ネットワークインターフェースは、スイッチ部300から出力されたパケットを、パケットの先頭にあるトンネル出口ラベルを用いて、ラベルスイッチングする。

【0139】一方、ノードがパケットをネットワークインターフェース部301から受信した場合に、パケットが自ノード宛である場合には、以下の処理を行う。

【0140】まず、ペイロードが上位プロトコルレイヤパケットであれば、パケットを中央処理部302に送信し、そうでなければ、セキュリティデータベース（SD）を参照し、SA情報および処理すべき内部処理インターフェース部303を決定した後、受信パケットのペイロード、SAラベル値（受信パケットがSAラベルを持たなければNULL値となる）を、スイッチ部300を通して決定した内部処理インターフェース部303に送信する。内部処理インターフェース部303では、必要であればペイロードをSPで復号化処理後、復号化後のペイロード（＝暗号化前のPDU）の先頭部に存在する暗号化前のパケットヘッダの情報またはMPLSヘッダの情報を元に内部処理インターフェース部303内のFWを参照して、指定された宛先アドレスに対する出力ネットワークインターフェース部を決定し、スイッチ部300を通して出力ネットワークインターフェース部に送信する。出力ネットワークインターフェースは、スイッチ部300から出力された復号化後のペイロード（＝暗号化前のPDU）、レイヤ2処理を行った後、これを外部に出力する。

【0141】（第6実施形態）以下に本発明の第6実施形態を説明する。図17に本実施形態で用いられる暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノードとネットワーク的に接続する装置として配置した場合のハード構成の一例を示す。

【0142】図17において、暗号処理ノードは、スイッチ部400、ネットワークインターフェース部401、および、中央処理部（CPU+Mem）402から構成される。なお、スイッチ部400を用いるかわりに、内部パスを用いることにより、スイッチ部、ネットワークインターフェース部、内部処理インターフェース部および、中間処理部間のデータ転送を実現してもよい。また、暗号処理ノードは、セキュリティ処理インターフェース403を介して、イーサネット404上にイーサスイッチ405を介して接続するセキュリティプロセッサ（SP）406に接続される。

【0143】イーサスイッチ405は、ラベルスイッチング機能を持っていてもよい。このとき、ノードからセキュリティプロセッサ（SP）406に送られるパケットは、MPLSヘッダをもち、かつ、そのパケットが含まれるイーサネットフレームの宛先アドレスは、イーサスイッチ405のMACアドレスとなる。

【0144】各ネットワークインターフェース部401はセキュリティデータベース（SD）およびフォワーディングテーブル（FW）を持つ。中央処理部402は、自ノード宛のIPパケットのうちペイロードがIPのPDUでないもの（IP-in-IPでないもの）に対する処理および、FW，SD，SPの管理を行う。

【0145】ノードは、パケットをネットワークインターフェース部401から受信した場合には、まず、受信パケットのIPヘッダまたはMPLSヘッダの情報からパケットが自ノード宛かどうかを調べ、一致しない場合には、以下の処理を行う。

【0146】まず、ネットワークインターフェース部401内のFWを参照してトンネル出口を決定する。次に、セキュリティデータベース（SD）を参照し、パケットに対してセキュリティ処理を行わない場合には、スイッチ部400経由でトンネル出口に対する出力インターフェースにパケットを出力する。パケットに対して暗号化処理を行う場合には、SA、および処理すべきセキュリティプロセッサ（SP）406を決定した後、トンネル出口用ラベルスタックエントリ、SA用ラベルスタックエントリの順にパケットのペイロードにプッシュして、これをスイッチ部400を通してセキュリティ処理インターフェース403に送信する。セキュリティ処理インターフェース403は、SA用ラベルスタックエントリを参照して、イーサスイッチ405経由で所定のセキュリティプロセッサ（SP）406にパケットをイーサネット（登録商標）フレーム化して送信する。

【0147】イーサスイッチ405は、ラベルスイッチング機能を有する場合でかつ、自ノード宛のMPLSヘッダ付きのパケットを受信すると、先頭のラベルスタックエントリを参照して所定のセキュリティプロセッサ（SP）406にパケットをフォワードする。ラベルスイッチング機能を有しない場合には、単に通常のイーサスイッチとして動作する。

【0148】セキュリティプロセッサ（SP）406では、パケットの先頭のラベルスタックをポップし、ポップしたラベルスタックエントリ中のSAラベル値を参照してパケットを暗号化処理後、SAラベル値を参照して暗号化後のパケットをノードに返す。ノードは、このパケットの先頭のラベルスタックエントリを参照して、トンネル出口ノードに対してパケットを送信する。

【0149】一方、ノードがパケットをネットワークインターフェース部401から受信した場合に、パケットが自ノード宛である場合には、以下の処理を行う。

【0150】まず、先頭のラベルスタックをポップする。結果として得られたパケットが上位プロトコルレイヤパケットであれば、パケットを中央処理部402に送信し、そうでなければ、セキュリティデータベース（SD）を参照し、SA情報および処理すべきセキュリティプロセッサ（SP）406を決定した後、次のラベルスタックエントリを参照する。エントリ中のラベルがSAラベルでなければ、このラベル値をもとに通常のラベルスイッチングによりパケットを転送する。SAラベルであれば、パケットを、スイッチ部400を通してセキュリティ処理インターフェース403に送信する。セキュリティ処理インターフェース403は、SA用ラベルスタックエントリを参照して、イーサスイッチ405経由で所定のセキュリティプロセッサ（SP）406にパケットをイーサネットフレーム化して送信する。

【0151】イーサスイッチ405は、ラベルスイッチング機能を有する場合でかつ、自ノード宛のMPLSヘッダ付きのパケットを受信すると、先頭のラベルスタックエントリを参照して所定のセキュリティプロセッサ（SP）406にパケットをフォワードする。ラベルスイッチング機能を有しない場合には、単に通常のイーサスイッチとして動作する。

【0152】セキュリティプロセッサ（SP）406では、パケットの先頭のラベルスタックエントリをポップし、この情報を元にペイロードを復号化処理後、復号化後のペイロード（＝暗号化前のPDU）をノードに返す。ノードは、受信したパケットがIPヘッダを持てばパケットをIP転送し、MPLSヘッダを持てばパケットをラベルスイッチングする。

【0153】以上、上記した実施形態によれば、1つのノードがIPカプセル化あるいは、MPLSのLSPで実現される複数のVPNをサポートする場合でも、MPLSセキュリティ機能をサポートすることができる。

【0154】また、トンネルの入り口でMPLSのラベルを含むパケットをレイヤ3パケットにカプセル化しているので、単なるIPカプセル化の場合に比べてカプセル化ノードにおいて、宛先アドレスに関するベストマッチ検索の回数を2回から1回に減らすことができる。

【0155】レイヤ3テーブルを2回検索する必要がなくなり、検索によるルータの付加を軽減できる。

【0156】また、セキュリティ処理が必要であることを示すSAラベルと、セキュリティ処理が必要でないラベルの値が重複しないようにしたので、暗号化パケットと非暗号化パケットの識別が可能となる。

【0157】また、ノードがレイヤ3パケットを暗号化して送信する場合には、セキュリティアソシエーションに関する情報を含むラベルスタックエントリに対してはラベルスタックの最後のラベルスタックエントリであることを示すフラグをオンにし、ノードがMPLSパケットを暗号化して送信する場合には、ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオフにする。これによって、MPLSパケットとレイヤ3パケットの両方を暗号化してMPLSパケットとしてVPNトンネル上でラベルスイッチングすることが可能になる。

【0158】また、SAラベル値を参照して、ラベル値が異なるパケットは異なる暗号処理プロセッサで並列処理を行うようにしたので、トラヒックの負荷が高い場合に並列処理を行わない場合に比べて暗号処理の高速化が可能となる。

【0159】さらに、暗号処理プロセッサは暗号化パケット処理ノード内に存在せず、ネットワーク的に暗号化パケット処理ノードと接続することが可能となるため、スケーラブルかつフレキシブルな暗号処理ノードの構成が可能となる。

【0160】また、復号側ノードでは、パケットを暗号処理するかどうかの判定、暗号処理する場合には使用されるセキュリティアソシエーションの決定、暗号処理しない場合にはどのノードにパケットをフォワードするかの決定、がすべてラベル値を参照することにより行われるため、パケット処理の一元化および高速化が可能となる。

【0161】

【発明の効果】請求項1～10に記載の発明によれば、1つのノードがIPカプセル化あるいは、MPLSのLSPで実現される複数のVPNをサポートする場合でも、MPLSセキュリティ機能をサポートすることができる。

【0162】また、請求項3に記載の発明によれば、セキュリティ処理が必要であることを示すSAラベルの値と、セキュリティ処理が必要でないラベルの値が重複しないようにしたので、暗号化パケットと非暗号化パケットの識別が可能となる。

【0163】また、請求項4に記載の発明によれば、MPLSパケットとレイヤ3パケットの両方を暗号化してMPLSパケットとしてVPNトンネル上でラベルスイッチングすることが可能になる。

【0164】また、請求項5に記載の発明によれば、SAラベル値を参照して、ラベル値が異なるパケットは異なる暗号処理プロセッサで並列処理を行うようにしたので、トラヒックの負荷が高い場合に並列処理を行わない場合に比べて暗号処理の高速化が可能となる。

【0165】また、請求項6に記載の発明によれば、ネットワーク的に暗号化パケット処理ノードと接続することが可能になるため、スケーラブルかつフレキシブルな暗号処理ノードの構成が可能となる。

【0166】また、請求項11及び12に記載の発明に

よれば、カプセル化ノードにおいて、宛先アドレスに関するベストマッチ検索の回数を２回から１回に減らすことができる。

【図面の簡単な説明】

【図１】１つのノードがＩＰカプセル化で１つ以上のＶＰＮを構築する場合のネットワークの構成を示す図である。

【図２】ＩＰカプセル化による暗号化処理を行うＶＰＮの一例を示す図である。

【図３】ＭＰＬＳのフォーマットを示す図である。

【図４】ＭＰＬＳを用いた暗号化処理を行うＶＰＮの一例を示す図である。

【図５】ＩＰネットワークとＭＰＬＳネットワークとが混在した場合のネットワーク構成を示す図である。

【図６】ＩＰ，ＭＰＬＳ処理方式のいずれかを選択する工程を示すフローチャートである。

【図７】ＶＰＮエッジルータが、ＩＰパケットを受信した場合の処理を説明するためのフローチャートである。

【図８】本実施形態のＶＰＮエッジルータが、ＭＰＬＳのラベル化パケットを受信した場合の処理を説明するためのフローチャートである。

【図９】暗号側処理１の詳細を説明するためのフローチャートである。

【図１０】復号側処理１の詳細を説明するためのフローチャートである。

【図１１】暗号側処理２の詳細を説明するためのフローチャートである。

【図１２】復号側処理２の詳細を説明するためのフローチャートである。

【図１３】本実施形態で用いられるセキュリティデータベースの構成を示す図である。

【図１４】本実施形態におけるＶＰＮトンネル上を転送されるパケットのパケットフォーマットを示す図である。

【図１５】図7から図１２に示すフローチャートの処理を実現するノードのブロック図である。

【図１６】本実施形態で用いられる暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノード内に配置した場合のハード構成の一例を示す図である。

【図１７】本実施形態で用いられる暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノードとネットワーク的に接続する装置として配置した場合のハード構成の一例を示す図である。

【図１８】ＩＰＳＥＣゲートウェイ（ＩＰＳＥＣ－ＧＷ）によるＩＰＳＥＣ処理の仕組みを示す図である。

【図１９】ＩＰＳＥＣ用のＳＡ確立と鍵交換にかかわるＩＳＡＫＭＰ（Internet Security Association and Key Management Protocol ）を示す図である。

【図２０】トランスポートモードとトンネルモードの各々における、ＩＰパケット中のＡＨおよびＥＳＰヘッダ位置と、認証／暗号化範囲を示す図である。

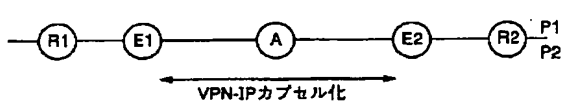
【図２１】ＡＨ（Authentication Header ）の構造を示す図である。

【図２２】ＥＳＰ（Encapsulating Security Payload）の構造を示す図である。

【符号の説明】

Ｅ１，Ｅ２…ＶＰＮエッジルータ（暗号化ルータ）、
Ｒ１，Ｒ２…ラベルスイッチエッジルータ、
ＳＰ１，ＳＰ２…セキュリティプロセッサ、
ＳＷ…ラベルスイッチ、
１００…Ｌ２ヘッダ、
１０１…シムヘッダ、
１０２…Ｌ３ヘッダ、
１０３…Ｌ４ヘッダ、
１０４…データ、
１０５…ラベル、
１０６…エクスペリメンタルユースビット、
１０７…Ｓフラグ、
１０８…ＴＴＬビット
２００…自ノード宛パケット処理部、
２０１…パケット入力部、
２０２…ＩＰ／ＭＰＬＳヘッダ解析部、
２０３…復号処理部、
２０４…セキュリティデータベース（ＳＤ）、
２０５…暗号化側セキュリティポリシー決定部、
２０６…暗号処理部、
２０７…復号化側セキュリティポリシー決定部、
２０８…ＩＰ／ＭＰＬＳパケットフォワーディング処理部、
２０９…パケット出力部。

【図２】

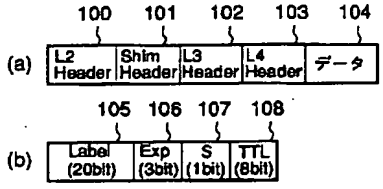


R1, R2：ラベルスイッチエッジルータ
E1, E2：暗号化ルータ
A：ISPのルータ

【図１３】

ﾄﾝﾈﾙ出口	ｾﾚｸﾀ	ﾎﾟﾘｼｰ	SPI	ｾｷｭﾘﾃｨﾌﾟﾛﾄｺﾙ／
				ｱﾙｺﾞﾘｽﾞﾑ／鍵
	送信元ｱﾄﾞﾚｽ=H11	暗号化	100	ESP/A1/K1
E2	送信元ｱﾄﾞﾚｽ=H12	暗号化	200	ESP/A2/K2
	その他	非暗号化		
その他	指定なし	廃棄		

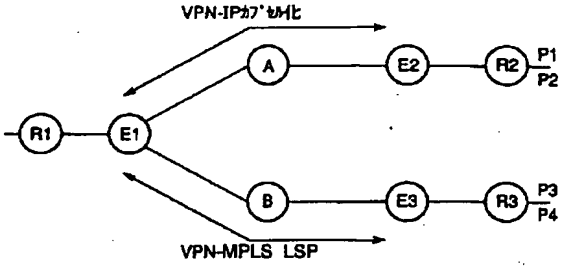
【図1】



Label : Label Value, 20bits
Exp : Experimental Use, 3bits
S : Bottom of Stack, 1bit
TTL : Time to Live, 8bits

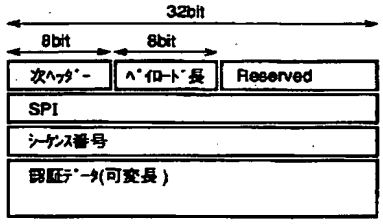
1. Label Value
2. Experimental Use
   Experimental Useであり、未定義
3. Bottom of Stack (S)
   Label Stackの最後のEntry(Bottom Label Stack)の場合、
   "1" を設定する
   Bottom Label Stackでなければ、 "0" を設定する
4. Time to Live (TTL)
   TTLをEncodeする

【図5】



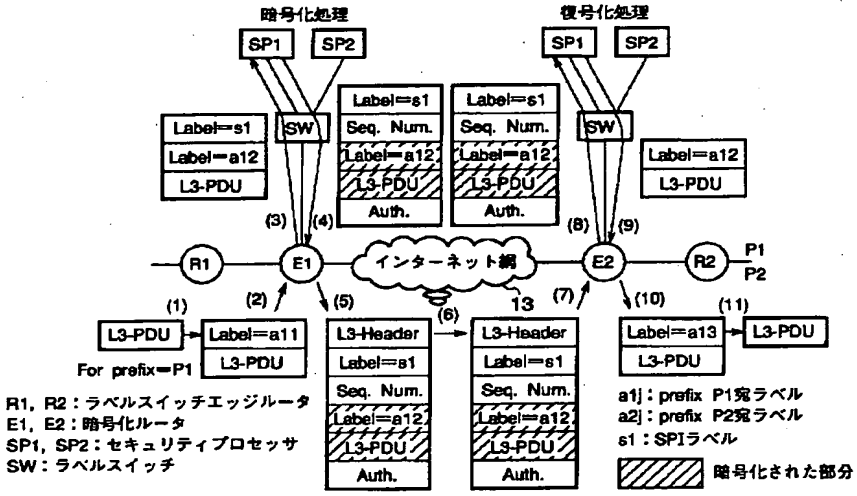
R1, R2, R3 : ラベルスイッチエッジルータ
E1, E2, E3 : 暗号化ルータ
A, B : ISPのルータ

【図21】



・次ヘッダー：認証データの次に来るプロトコル番号
・シーケンス番号：リプレイ攻撃を阻止するため、
各パケットに順序番号を付ける

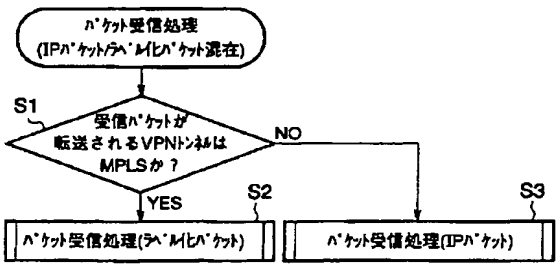
【図3】



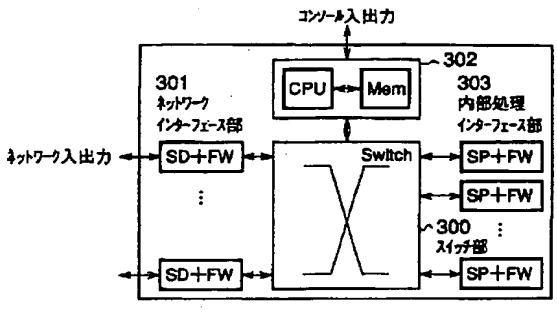
R1, R2 : ラベルスイッチエッジルータ
E1, E2 : 暗号化ルータ
SP1, SP2 : セキュリティプロセッサ
SW : ラベルスイッチ

a1] : prefix P1宛ラベル
a2] : prefix P2宛ラベル
s1 : SPIラベル
暗号化された部分

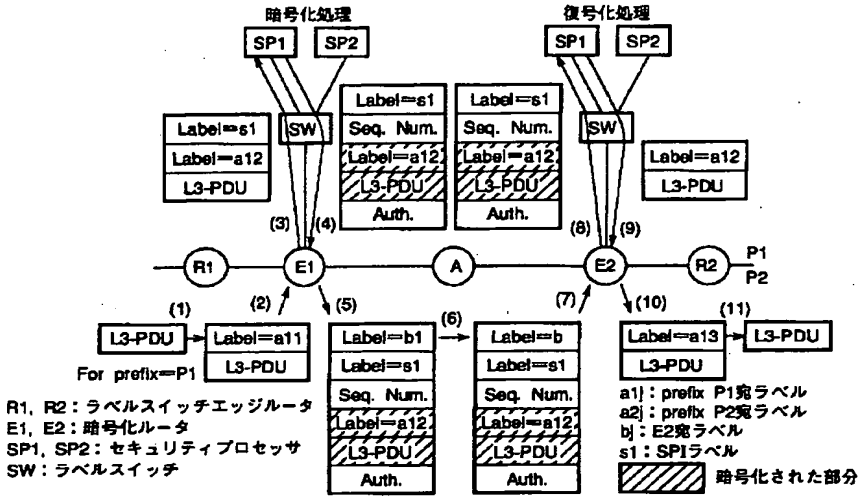
【図6】



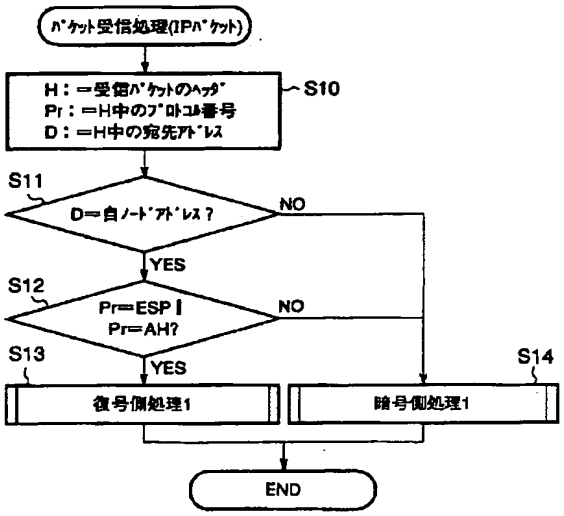
【図16】



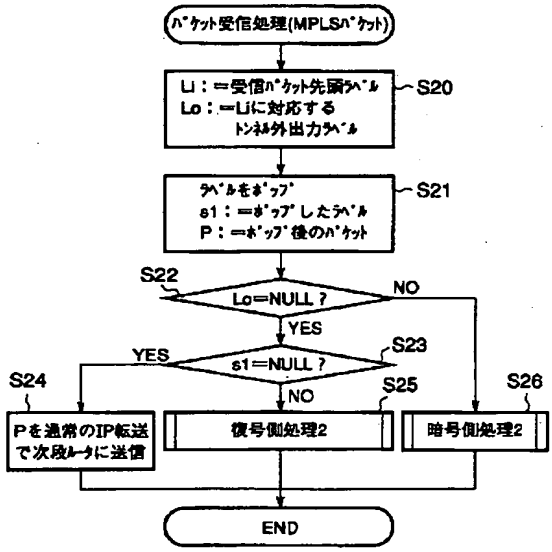
【図4】



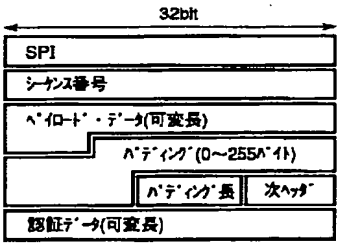
【図7】



【図8】

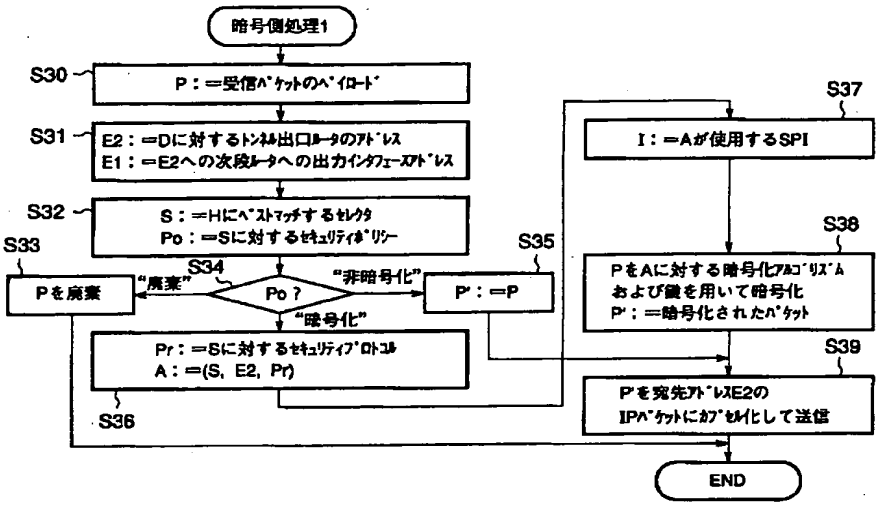


【図22】

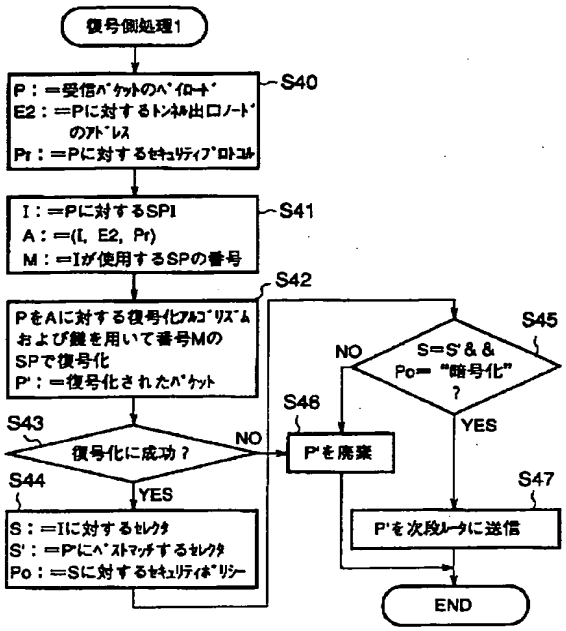


・SPI：SPI値と宛先IPｱﾄﾞﾚｽで該当するSAを一意に指定する
・ｼｰｹﾝｽ番号：ﾘﾌﾟﾚｲ攻撃を阻止するために順序番号を付ける
・ﾊﾟﾃﾞｨﾝｸﾞ：ﾊﾟｹｯﾄ長を調整するためのﾊﾟﾃﾞｨﾝｸﾞ・ﾃﾞｰﾀ
・認証ﾃﾞｰﾀ：ESPﾍｯﾀﾞ、暗号鍵、ﾍﾟｲﾛｰﾄﾞをﾊｯｼｭ化したﾃﾞｰﾀ

【図9】



【図10】



【図14】

トンネルPDU(IPv4)：＝ﾚｲﾔ2ﾍｯﾀﾞｰ＋［LSE＋…］＋LSE＋
［ESP‖SPIなしESP‖IPv4ﾊﾟｹｯﾄ］
トンネルPDU(IPv6)：＝ﾚｲﾔ2ﾍｯﾀﾞｰ＋［LSE＋…］LSE＋
［ESP［＋IPv6拡張ﾍｯﾀﾞｰ＋］‖SPIなしESP
［＋IPv6拡張ﾍｯﾀﾞｰ］‖IPv6ﾊﾟｹｯﾄ］

LSE：＝ﾗﾍﾞﾙ(20bits)＋Exp(3bits)＋S(1bits)＋TTL(8bits)

SPIなしESP：＝ｼｰｹﾝｽ番号(4octets)＋ﾍﾟｲﾛｰﾄﾞﾃﾞｰﾀ(可変長)＋
ﾊﾟﾃﾞｨﾝｸﾞ(0～255octets)＋ﾊﾟﾃﾞｨﾝｸﾞ長(1octet)＋
次ﾍｯﾀﾞｰ(1octet)＋認証ﾃﾞｰﾀ(可変長)

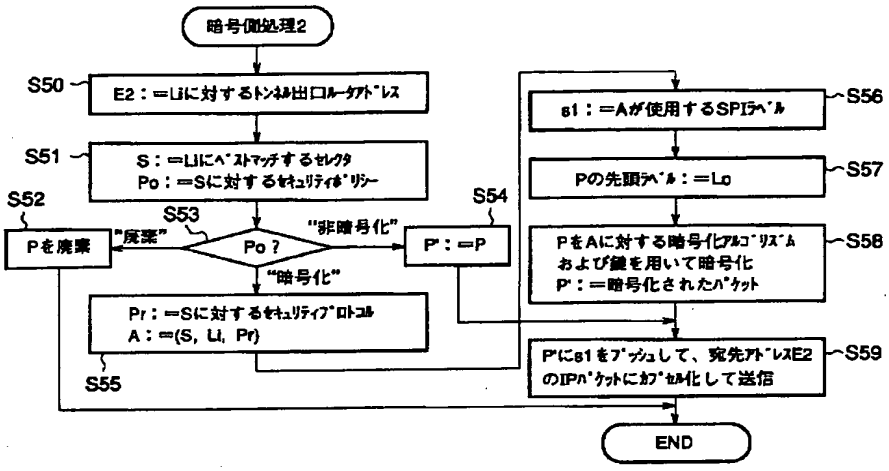
ESP：＝SPI＋SPIなしESP

ﾍﾟｲﾛｰﾄﾞﾃﾞｰﾀ：＝Encrypt(暗号化前ﾍﾟｲﾛｰﾄﾞﾃﾞｰﾀ)

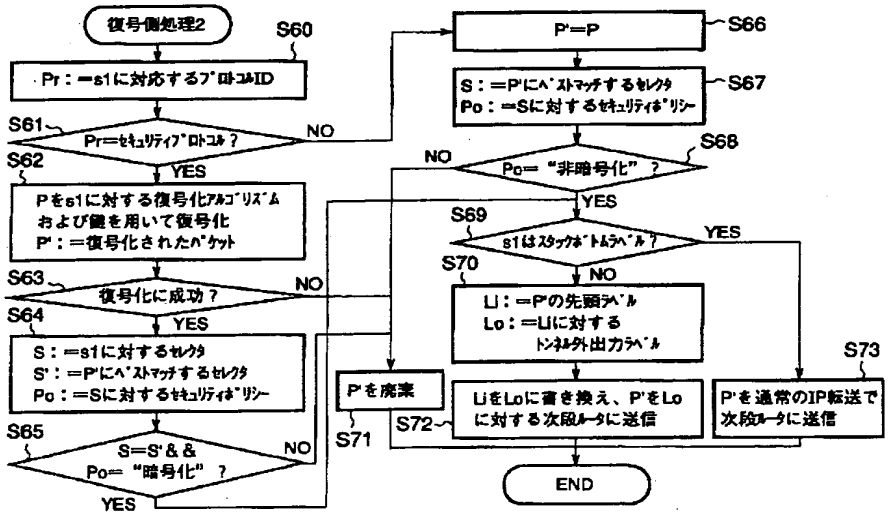
暗号化前ﾍﾟｲﾛｰﾄﾞ：＝｛IPﾊﾟｹｯﾄ‖［LSE＋…］＋LSE＋IPﾊﾟｹｯﾄ｝

LSE：Label Stack Entry
ESP：Encapsulating Security Payload
SPI：Security Parameter Index
Exp：Experimetal Field
TTL：Time To Live

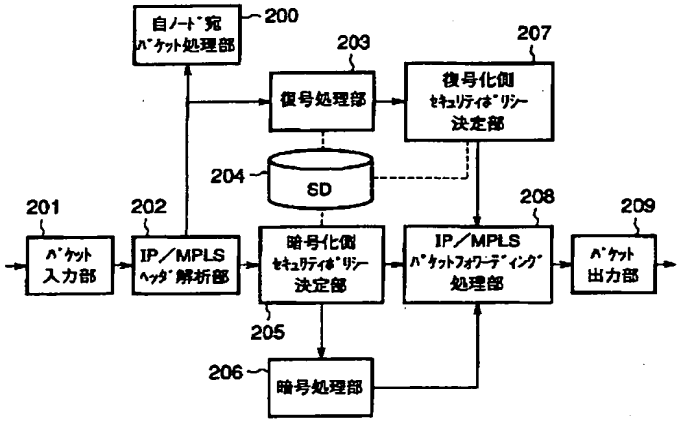
【図11】


暗号側処理2
S50
E2：＝Liに対するﾄﾝﾈﾙ出口ﾙｰﾀｱﾄﾞﾚｽ
S51
S：＝Liにﾍﾞｽﾄﾏｯﾁするｾﾚｸﾀ
Po：＝Sに対するｾｷｭﾘﾃｨﾎﾟﾘｼｰ
S52
S53
S54
Pを廃棄
"廃棄"
Po？
"非暗号化"
"暗号化"
P'：＝P
Pr：＝Sに対するｾｷｭﾘﾃｨﾌﾟﾛﾄｺﾙ
A：＝(S, Li, Pr)
S55
s1：＝Aが使用するSPIﾗﾍﾞﾙ
S56
Pの先頭ﾗﾍﾞﾙ：＝Lo
S57
PをAに対する暗号化ｱﾙｺﾞﾘｽﾞﾑ
および鍵を用いて暗号化
P'：＝暗号化されたﾊﾟｹｯﾄ
S58
P'にs1をﾌﾟｯｼｭして、宛先ｱﾄﾞﾚｽE2
のIPﾊﾟｹｯﾄにｶﾌﾟｾﾙ化して送信
S59
END

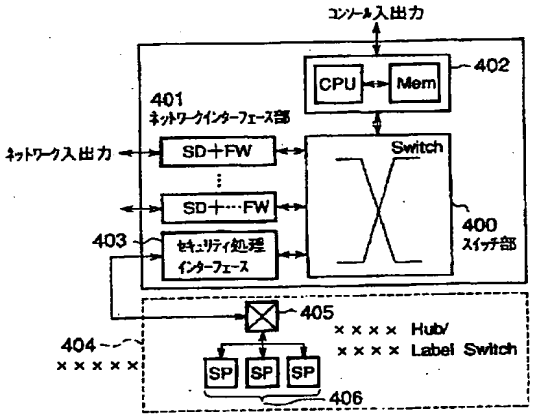
【図12】


復号側処理2
S60
Pr：＝s1に対応するﾌﾟﾛﾄｺﾙID
S61
Pr＝ｾｷｭﾘﾃｨﾌﾟﾛﾄｺﾙ？
NO
YES
S62
Pをs1に対する復号化ｱﾙｺﾞﾘｽﾞﾑ
および鍵を用いて復号化
P'：＝復号化されたﾊﾟｹｯﾄ
S63
復号化に成功？
NO
YES
S64
S：＝s1に対するｾﾚｸﾀ
S'：＝P'にﾍﾞｽﾄﾏｯﾁするｾﾚｸﾀ
Po：＝Sに対するｾｷｭﾘﾃｨﾎﾟﾘｼｰ
S65
S=S'＆＆
Po＝"暗号化"？
NO
YES
P'=P
S66
S：＝P'にﾍﾞｽﾄﾏｯﾁするｾﾚｸﾀ
Po：＝Sに対するｾｷｭﾘﾃｨﾎﾟﾘｼｰ
S67
S68
NO
Po＝"非暗号化"？
YES
S69
s1はｽﾀｯｸﾎﾞﾄﾑﾗﾍﾞﾙ？
YES
NO
S70
Li：＝P'の先頭ﾗﾍﾞﾙ
Lo：＝Liに対する
ﾄﾝﾈﾙ外出力ﾗﾍﾞﾙ
S73
P'を廃棄
S71
LiをLoに書き換え、P'をLo
に対する次段ﾙｰﾀに送信
S72
P'を通常のIP転送で
次段ﾙｰﾀに送信
END

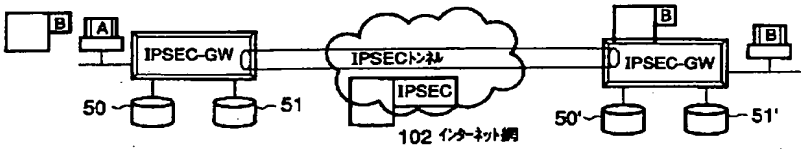
【図15】



【図17】



【図18】



セキュリティ・ポリシー・データベース

宛先アドレス	IPSEC処理	SA
B	やる	SA1
C	やる	SA2
D	やる	—
E	やらない	—

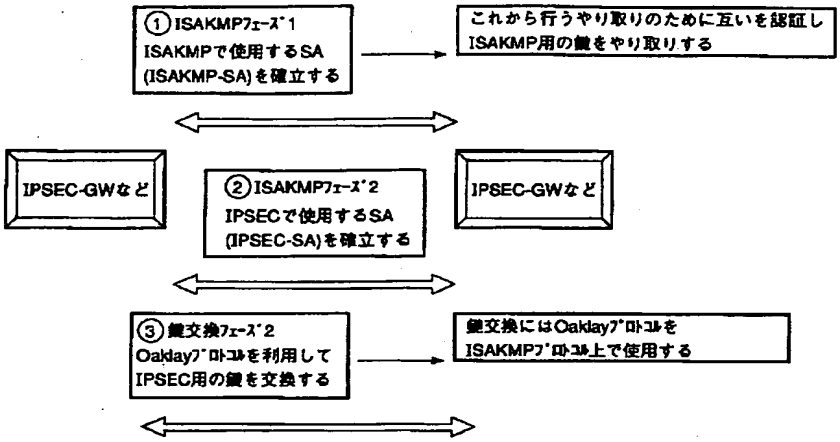
SAデータベース

SA2 SPI=2 宛先...

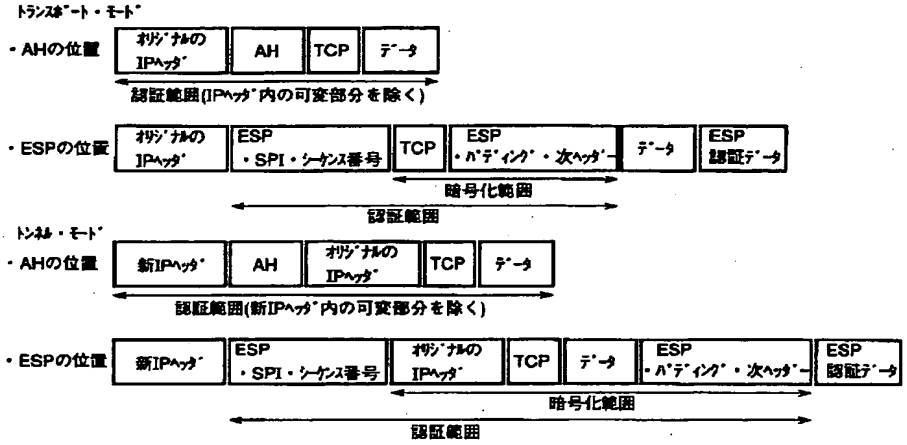
SA1 SPI=1 宛先...
ヘッダ=ESP
暗号鍵=＋＋＋
暗号アルゴリズム=DES
ヘッダ=AH
認証鍵
認証アルゴリズム=MD5
送信元アドレス
有効期限

SA：Security Association　SPI：Security Parameter Index　IPSEC-GW：Ipsec対応ゲートウェイ

【図19】



【図20】



フロントページの続き

(72)発明者　岸上　徹
東京都日野市旭が丘３丁目１番地の１　株式会社東芝日野工場内

Ｆターム(参考)　5J104 AA01 AA07 AA16 BA02 EA20
KA02 NA21 PA07
5K030 GA15 HA08 HC14 HD03
5K033 AA08 CC01 DB14 DB18 EC03